AMENDMENTS TO THE CLAIMS

1. (currently amended) A method of transmitting secured data, the method comprising:

utilizing a first key to encrypt a payload;

adding a header to the encrypted payload to form a data packet;

utilizing a second key to encrypt the first key;

utilizing a third key to encrypt the data packet;

transmitting the encrypted first key separate from the encrypted data packet to a wireline device in a first transmission from a wireless device, wherein the wireline device decrypts the encrypted first key;

transmitting only the encrypted data packet without said first key over a wireless link to a gateway in a second transmission from the wireless device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network; and

utilizing the wireline device and the first key from the first transmission to decrypt the encrypted payload.

2. (previously presented) The method of claim 1, wherein the first key comprises a symmetric key.

3. (previously presented) The method of claim 1, further comprising:

transmitting the encrypted first key to the wireline device, wherein the wireline

device decrypts the encrypted first key using a private key associated with the second key.

4. (previously presented) The method of claim 1, wherein the third key comprises a symmetric session key.

5. (canceled).

6. (currently amended) A device for transmitting secured data over a wireless link, the device comprising:

an encryption engine which generates a first key, encrypts a payload according to the first key, adds a header to the encrypted payload to form a data packet, encrypts the first key according to a second key, and encrypts the data packet according to a third key; and

a wireless transceiver coupled to the encryption engine, the wireless transceiver transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from the device and transmitting only the encrypted data packet without said first key over the wireless link to a gateway in a second transmission from the device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server over an open network;

wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload of the second transmission using the

decrypted first key.

7. (canceled).

8. (previously presented) The device of claim 6, wherein the payload comprises GPS location information obtained by the device and regarding a geographical location of the device.

9. (previously presented) The device of claim 6, wherein the first key comprises a symmetric key.

10. (currently amended) A method for secured communication between a mobile device and a server on a wide area network, the method comprising:

encrypting a payload at the mobile device using a first session key;

encrypting the first session key at the mobile device using a public key;

transmitting the encrypted first session key separate from an encrypted data packet to the server over a wireless link in a first transmission from the mobile device;

decrypting the encrypted first session key at the server;

adding a header to the encrypted payload to form a data packet at the mobile device;

encrypting the data packet according to a second session key configured for secured communications over the wireless link; and

transmitting only the encrypted data packet without said first key in a second

transmission from the mobile device to a gateway which decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server;

wherein the server utilizes the decrypted first session key, decrypted from the first transmission, to decrypt the encrypted payload.

11. (previously presented) The method of claim 10 wherein the decrypting the encrypted first session key at the server further comprises:

decrypting the encrypted first session key at the server using a private key associated with the public key.

12-14. (canceled).

15. (previously presented) The method of claim 10, wherein the payload includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device.

16. (previously presented) The method of claim 10, further comprising:

generating the first session key at the mobile device based on a random number.

17. (previously presented) The method of claim 10, wherein the encrypting the payload at the mobile device using the first session key further comprises:

encrypting the payload at the mobile device using the first session key, wherein

the first session key employs an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES.

18-19. (canceled).

20. (previously presented) The method of claim 1, further comprising:

implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES.

21-24. (canceled).

25. (previously presented) The method of claim 1, wherein the data packet includes GPS location information obtained by the wireless device and associated with a geographical location of the wireless device.

26. (previously presented) The method of claim 1, further comprising:

utilizing a random number to generate the first key.

27. (previously presented) The device of claim 6, further comprising:

a memory coupled to the encryption engine, wherein the memory stores the second key, and wherein the encryption engine accesses the second key from the memory.

28. (canceled).

29. (currently amended) A computer readable storage medium comprising program instructions for performing a method comprising:

encrypting a payload according to a first key;

adding a header to the encrypted payload to form a data packet;

encrypting the first key according to a second key;

encrypting the data packet according to a third key configured for secured communications over a wireless link;

transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from a mobile device; and

transmitting only the encrypted data packet without said first key over the wireless link to a gateway in a second transmission from the mobile device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server, and wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload using the decrypted first key.

30. (previously presented) The computer readable storage medium of claim 29, wherein the first key comprises a symmetric key.

31. (previously presented) The computer readable storage medium of claim 29, wherein the method further comprises:

receiving the data packet at the gateway;

decrypting the data packet at the gateway according to the third key;

forwarding the encrypted payload to the server;

receiving the encrypted first key at the server;

decrypting the encrypted first key using a fourth key; and

decrypting the payload according to the decrypted first key.

32. (previously presented) The computer readable storage medium of claim 29, wherein the first key comprises a symmetric session key.

33. (previously presented) The computer readable storage medium of claim 29, wherein the method further comprises:

implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES.

34. (previously presented) The computer readable storage medium of claim 29, wherein the data packet includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device.

35. (previously presented) The computer readable storage medium of claim 32, wherein the symmetric session key is generated based on a random number.